Anthony Shawn Bandy

Engineering 350

Monday 2:00PM

Writing Assignment 2

02/17/2013

Botnets[[1]](#footnote-1)

In its broadest meaning a Botnet is a network of programs cooperating to achieve one or more objectives, particularly in situations where a single program may be inadequate. Wikipedia refers to Botnets on Internet Relay Chat (IRC) as one example of early, legal Botnets. In this case Botnets would monitor IRC channels and boot users who were not conforming to the channel’s policies (i.e. the use of foul language).[[2]](#footnote-2) Quora, an internet question and answers service, also lists projects such as seti@home and Panda Anti-Virus Software as other examples of legal Botnet software.[[3]](#footnote-3) In most cases, however, the term Botnet implies a network of programs that cooperates for illicit and illegal purposes.

The crux of illegal Botnets lies in the cooption of unassuming personal computers. Usually this is carried out by infecting the target computer with a virus or worm where the payload is the bot software. The infected PC is then a *zombie* which is *herded* by a *master.* The zombie can be instructed to perform tasks such as sending out spam email, to participate in *click-fraud* or a distributed denial-of-service attack (DDOS). *Click-fraud* entails sending HTTP requests to a server that is monitor click-thrus in such a way that it mimics a human clicking on a link in a browser. Because some advertising hosts will pay per click, a Botnet acting in this capacity can generate revenue for its owner. A Botnet sending spam works in a similar way: when its recipients click on an email, the advertiser or site-owner will pay out small amounts. If the Botnet is relatively large these small payments can amount to substantial sums. A Botnet participating in or carrying out a DDOS attack disrupts internet traffic to and from its target. Although a DDOS attack is sometimes financially motivated, it can be politically motivated as well.

The general pattern for disabling a Botnet is to “cut the head off the snake.”[[4]](#footnote-4) Each node in the Botnet must in someway coordinate with other nodes and receive further instructions from the master. Very often, Botnets are hardcoded with the means to coordinate and receive instructions and, so, removing this mechanism from action effectively disables the network. Some newer Botnet software has shifted to more flexible and reliable pier-to-pier communication.[[5]](#footnote-5)

Gozi Virus

In 2005 a Russian national named Nikita Kuzman created the design requirements for a virus that would steal banking information from the users of infected computers. For example, the virus posed as a .pdf document that when opened infected the host computer with software that was designed to evade anti-virus software detection. He paid an individual referred to as CC-1 to do the initial development of the software and later paid others such as Deniss Calovskis, a Latvian national, to refine the software. Calovskis created “web injections” which were designed to glean additional information from its victims that would be required to fraudulently access their accounts. In addition to the revenue from fraudulently accessing the victims’ online bank accounts, Kuzman rented out the services of his virus network to others. A third individual, a Romanian named Ionut Panescu, provided the internet infrastructure for Kuzman to carryout his activities in a way that was difficult for authorities to pin-point. These three individuals were indicted by the United States Attorneys for the Southern District of New York; Kuzman has pled guilty.

Cezar Butu

Between 2009 and 2011, Cezar Butu along with other Romanian nationals worked on a scheme to steal credit card information from merchants in the United States. Butu, et al. “hacked” into merchants’ computer systems and retrieved “credit payment information” with which they made charges to and transferred funds from. He also sold some of the information to third parties in return for payments. Butu and one co-conspirator pled guilty; one remaining co-conspirator will go to trial later this week, on February 20th.

Vladimir Zdorovenin

Vladimir Zdorovenin and his son pled guilty to orchestrating “a series of sophisticated international cyber crimes.”[[6]](#footnote-6) The Zdorovenin’s used fake websites, stolen credit card information and bank accounts to steal money from U.S. citizens between 2004 and 2005. Although the details are sparse, it appears that Zdorovenin used similar techniques to those involved with the Gozi Virus and Cezar Butu’s group. Additionally he set up at least three firms expressly for the purposes of processing credit card purchases made with the stolen information in a way that evaded detection by banks, credit card processors and the card holders. He also created a firm with which he bought and sold securities using his victims’ financial data. Zdorovenin will be required to pay one million dollars in fines, an undetermined amount in restitution and three years in jail.

1. I will use *Botnet* and *Bot Net* interchangeably. [↑](#footnote-ref-1)
2. http://en.wikipedia.org/wiki/Botnet#Legal\_botnets [↑](#footnote-ref-2)
3. http://www.quora.com/What-are-some-good-examples-of-legal-botnets [↑](#footnote-ref-3)
4. http://blog.rjssoftware.com/tag/botnet/ [↑](#footnote-ref-4)
5. http://en.wikipedia.org/wiki/Botnet#Countermeasures [↑](#footnote-ref-5)
6. http://www.justice.gov/usao/nys/pressreleases/January13/ZdoroveninSentencingPR.php [↑](#footnote-ref-6)